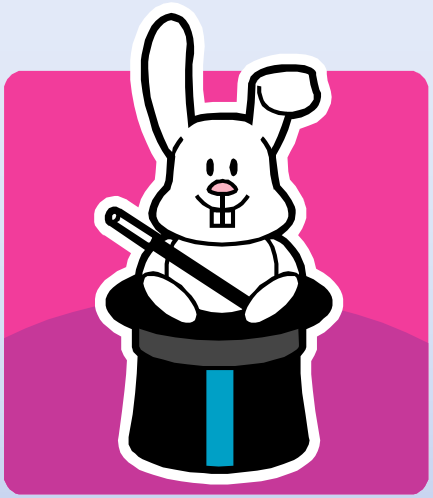
Current Security Threats

2011 Montana Government
Information Technology Conference
December 8, 2011

Presented by:
Lynne Pizzini, CISSP, CISM, CIPP
Information Systems Security Officer
State Information Technology Services Division
444-9127
lpizzini@mt.gov



Lynne Pizzini, CISSP, CISM, CIPP
Lyn-nerd the Clown
Information Systems Security Officer
State Information Technology Services Division

Outline – Current Security Threats

- Advanced Persistent Threats (APT)
- Cloud Computing
- Mobile Devices
- Social Engineering
- Spear Phishing
- Whaling
- Insider
- Review

Advanced Persistent Threats (APT)

Don’t ignore them!

- Adaptable
- Move around the network
- Root themselves in systems
- Sophisticated
- Fool security tools
- stealthy

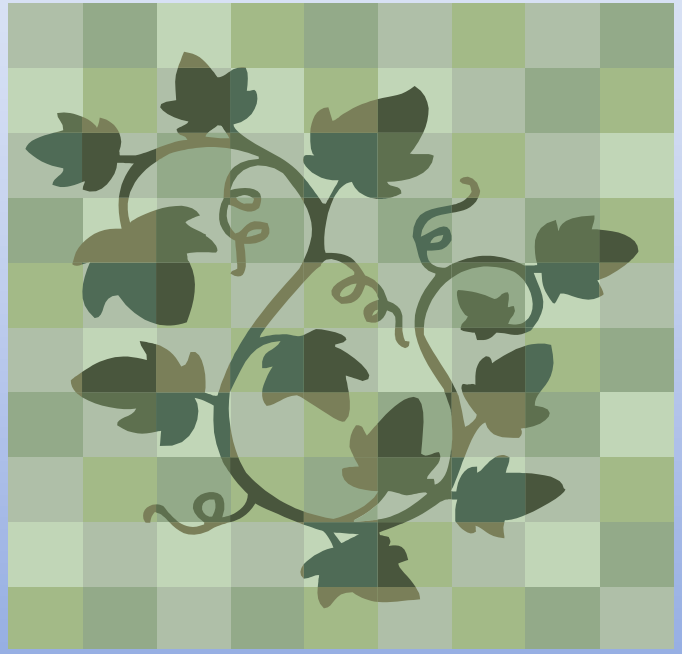
APT Attack on RSA

Started with 2 email messages with an attachment

Reconnaissance to collect information about systems

Attack was modified to fit the target environment

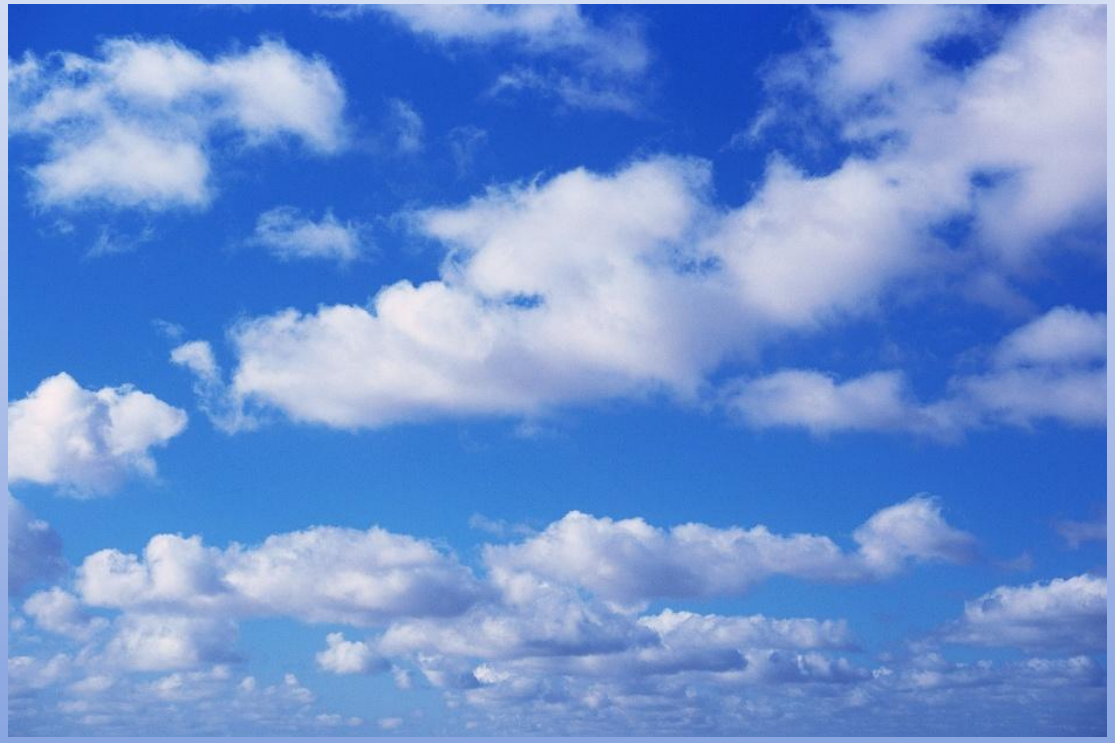
APT – Poison Ivy



A remote administration utility that bypasses normal security protections to secretly control a program, computer, or network.

Advanced Persistent Threats

Cloud Computing

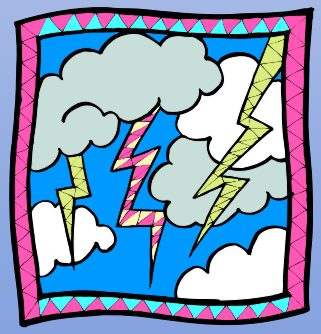


Risks

1. VENDOR SECURITY - Transparency vs. Secrecy
2. ISOLATION/SEGREGATION - Providers must ensure that multiple customers do not interfere with each other, maliciously or unintentionally
3. DATA LOCATION - Be sure your vendor contract stipulates any restrictions you may have on the physical location of where your data is stored such as other countries
4. MANAGEMENT INTERFACE - How is the system administered by the company – via the Internet? Do they use two factor authentication? Are administrators monitored?
5. REPUTATION SHARING - Bad behavior by one cloud customer may impact others using the cloud. For example a customer engaging in spamming may cause a common cloud IP address to be black listed.

Risks - Continued

5. PROVIDER VIABILITY - How long has the provider been in business? What happens to your organization's applications and data in the event that the provider goes out of business, is purchased by another business, or when the contract runs out?
6. COMPLIANCE - Placement of data in the cloud does not eliminate an organization's need to meet legal and regulatory requirements such as PCI or HIPAA.
7. DATA LOSS/LEAKAGE/CHANGED – Backup and recovery – timeline for restoration. How is information removed when equipment is replaced?
8. LOGGING – protection of audit logs. How can they be accessed for audit purposes?

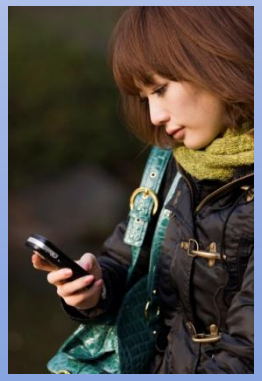


Risks - Continued

9. SECURITY INCIDENTS – incident management
10. Cloud Sprawl – unauthorized acquisition of cloud services

Cloud Computing Trick

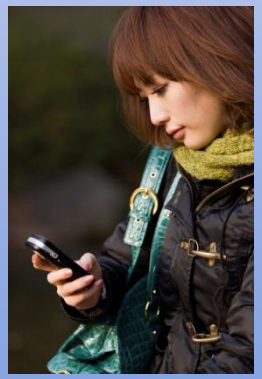
Mobile Devices



Management:

- Policy enforcement
- Authentication Control
- Remote Lock
- Remote Locate
- Remote wipe

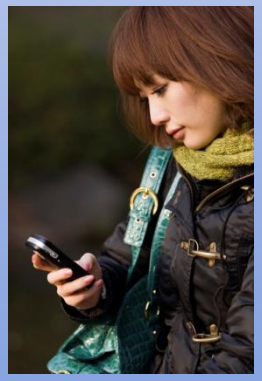
Mobile Devices



Security Controls:

- Patching
- Anti-virus/malware
- Firewall
- App control

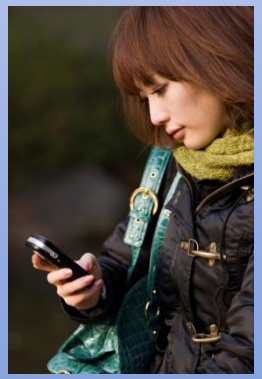
Mobile Devices



Other Concerns:

- Device replacement
- State data on personal devices
- Need for encryption
- Too many different devices to protect them all the same

Mobile Devices



Solution:

- Risk Assessment
- Policy and procedures

What is the Greatest Security Risk to Organizations Today?

EMPLOYEES!!!!!

This is the reason Education and Awareness is so important.

“Seven Times” Rule for Education

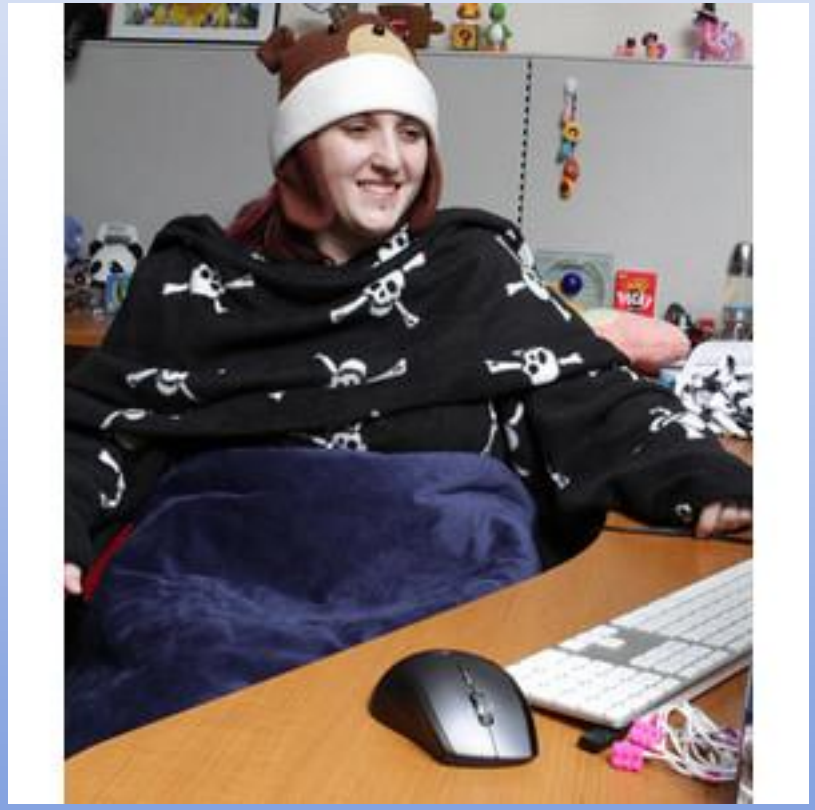
Greatest Security Risk

The Human Factor

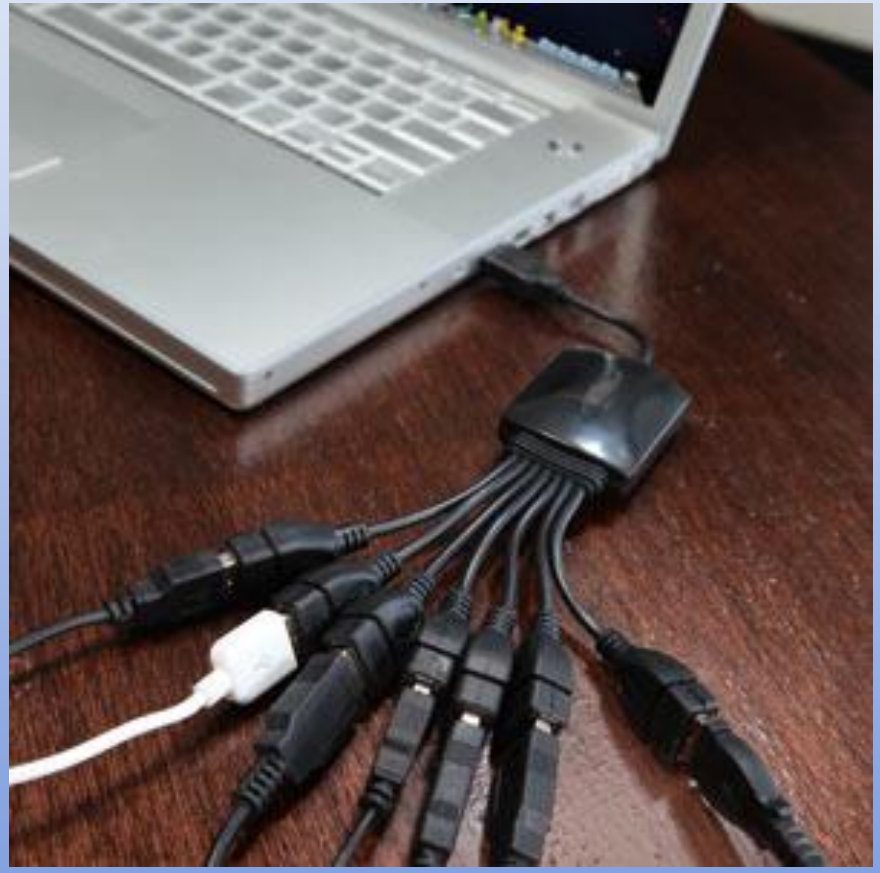
USB Devices

USB Devices

USB Devices



USB Devices



Social Engineering

The practice of obtaining confidential information by manipulating and/or deceiving people.

Examples of Social Engineering

Phishing Email or web site – bank, job layoff, something appealing

USB Stick

Telephone – Help Desk, System Administrator, Director

Examples of Social Engineering

- Your bank account has been compromised. Click here to get your money returned to you.
- I sent you some pictures of my family, click here.
- Someone has a secret crush on you! Download this application to find out who it is!
- Did you see this video of you? Check out this link!
- Click here to get coupons for free McDonalds meals.

Examples of Scial Engineering

- Your bank account has been compromised. Click here to get your money returned to you.
- I sent you some pictures of my family, click here.
- Someone has a secret crush on you! Download this application to find out who it is!
- Did you see this video of you? Check out this link!
- Click here to get coupons for free McDonalds meals.

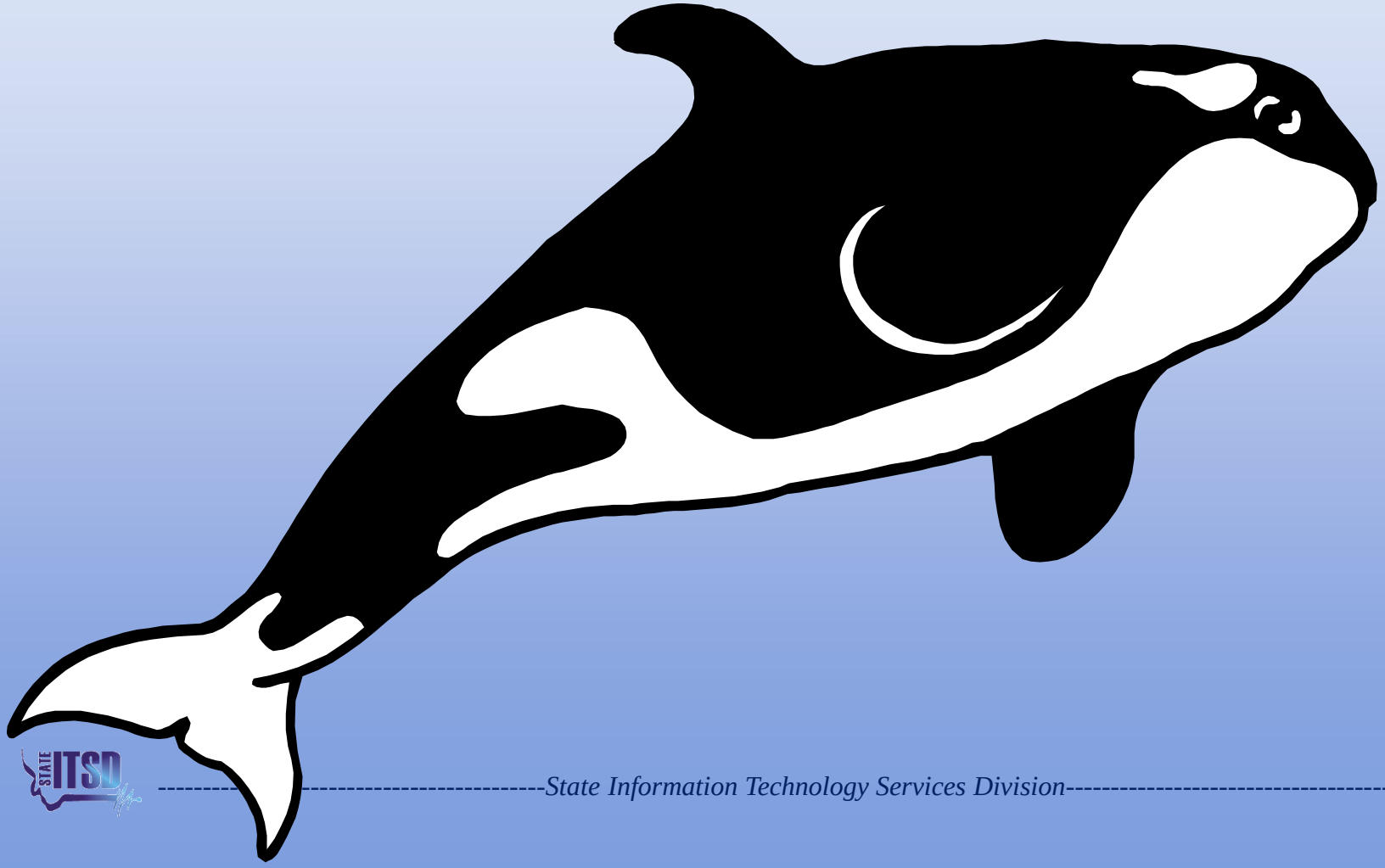
Spear Phishing – Target Phishing

- Email from trusted colleagues
- Email from Human Resources
- Email from bank

Top 10 Holiday Phishing Scams

1. Football – live streaming media
2. Secret Santa Gifts
3. I-tunes Gift Card
4. E-cards
5. Survey – Gift Card
6. QR (Quick Response) Code on Smart Phones
7. Direct Deposit did not work
8. Parcel has arrived at the Post Office, UPS, Fed-X – use postal label
9. Flight Confirmations
10. Holiday Screen Savers

Whaling

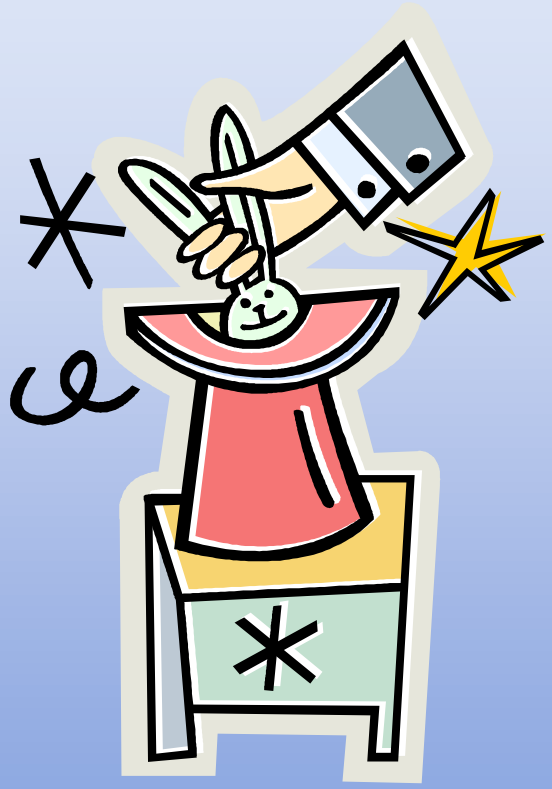


Insider Threat

- 43% of malicious attacks are insiders
- Insider incidents usually result in more damage
- 80% of successful malware threats required some human action

Human Firewall

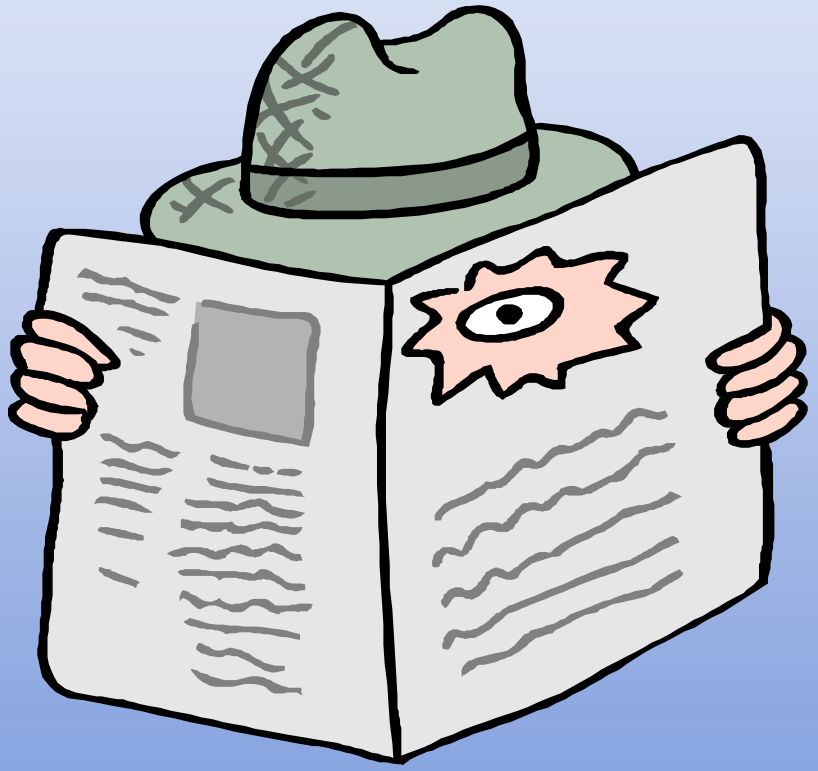
The Security Star



Resources

- CSO Magazine
- MS-ISAC
- NASTD Security Special Interest Group
- NetworkWorld
- ISACA
- SANS

Final Comment



Threats are always changing so keep an eye on your systems.

Final Trick

Summary

- Advanced Persistent Threats (APT)
- Cloud Computing
- Mobile Devices
- Social Engineering
- Spear Phishing
- Whaling
- Insider
- Review

ANY QUESTIONS?